0 = full scan

| L Number | Hits | Search Text | DB | Time stamp |
|---|---|---|---|---|
| - | 5 | ingrian.as. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 06:57 |
| - | 1 | ("6081900").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/27 09:44 |
| - | 15 | ingrian.as. | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/27 13:46 |
| - | 0 | (@ad<20000612 and (rsa same (efficien$3)) and (chinese)) and (hensle hensel) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/27 13:47 |
| - | 19 | @ad<20000612 and (rsa same (efficien$3)) and (chinese) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/30 09:22 |
| - | 386 | rsa and ("160" adj bits) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/28 10:16 |
| - | 27 | rivest.in. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/28 13:41 |
| - | 1 | "20020087884" | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/10/01 08:07 |
| - | 1 | ("4,242,117").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 07:29 |
| - | 8 | (boneh.in. shacham.in. beri.in.) and (rsa) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 07:40 |
| - | 7 | (minimiz$3 with (disparity difference) with exponents) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 07:41 |
| - | 316 | rsa and ((reduc$3 minimiz$5) with (prime p q)) and (m n modulus pq) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 07:43 |
| - | 100 | rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 07:43 |
| - | 45 | (rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612 | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 08:02 |
| - | 43 | ((rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612) and ("1/3" third three) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 08:13 |

| | | | | |
|---|---|---|---|---|
| - | 37 | ((rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612) and ("1/3" third ) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 08:02 |
| - | 23 | (((rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612) and ("1/3" third three)) not silverbrook.in. | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 08:14 |
| - | 6 | ((((rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612) and ("1/3" third three)) not silverbrook.in.) not (((rsa and ((reduc$3 minimiz$5) with (prime p q)) and ((m n modulus pq) with constan$5)) and @ad<20010612) and ("1/3" third )) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 08:14 |
| - | 0 | compaq.as. and (multi adj prime) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 09:40 |
| - | 18 | compaq.as. and rsa | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 09:40 |
| - | 0 | compaq.as. and rsa and ssl | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 09:46 |
| - | 1 | ("5848159").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:29 |
| - | 2 | ("4405829").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:30 |
| - | 1 | (("4405829").PN.) and (size bit lenght) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:30 |
| - | 799 | rsa and ((private adj key) same random) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:38 |
| - | 494 | rsa and ((private adj key) with random) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:38 |
| - | 521 | rsa and ((private adj key) with random$2) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:38 |
| - | 35 | @ad<20000612 and rsa same ((private adj key) with random$2) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:49 |
| - | 101 | @ad<20000612 and rsa same ((private adj key) with (length bit)) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:50 |
| - | 41 | @ad<20000612 and rsa same ((private adj key) with (length bit size)) and ("public key" with (length bit size)) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 10:50 |
| - | 5 | ((hensle hensel) adj lift$3) and rsa | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/29 11:15 |

| | | | | |
|---|---|---|---|---|
| - | 15 | hensel adj lift$3 | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB | 2004/09/29 15:44 |
| - | 1 | ("6735694").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 07:00 |
| - | 1 | ("5875296").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 07:46 |
| - | 1 | ("6085030").PN. | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:15 |
| - | 5 | session adj integrity adj key | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:15 |
| - | 919 | rsa and (bits near (long length)) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:48 |
| - | 67 | rsa and (bits near (long length)) and (chinese) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:49 |
| - | 45 | rsa and (bits near (long length)) and (chinese) and exponent | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:49 |
| - | 22 | rsa and (bits near (long length$2)) and (chinese) and (exponents roots) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 09:59 |
| - | 61 | rsa and (bits same (exponent$3 root$3)) and (chinese) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 10:00 |
| - | 5 | rsa and (bits same (exponent$3 root$3)) same (chinese) | USPAT; US-PGPUB; EPO; JPO; IBM_TDB | 2004/09/30 10:00 |

09877655
Michael J. Simitoski
Michael.Simitoski@uspto.gov
(703) 305-8191

## Google

rsa crt "160 bits"
chinese remainder "exists a unique element" pair rsa
"mod(p-1)" "mod(q-1)" crt rsa
addition subtraction multiplication division modulo arithmetic
rsa (CRT OR chinese) (hensle OR hensel) (lifting) ("1/3" OR third or 3)
multi-prime rsa
rsa ("chinese remainder" OR CRT) (hensle OR hensel) (efficient OR efficiency)
efficient rsa decryption (CRT OR chinese)
"Fast Implementation of RSA Cryptography"
"techniques for implementing the rsa public"
pkcs 8 (chinese OR crt) rsa (third OR "1/3")
pkcs 8 (chinese OR crt) rsa (third OR "1/3") multi-prime
RSA "chinese remainder" public private
rebalanced rsa
"Cryptanalysis of Short RSA Secret Exponents"
"chinese remainder theorem" ("hensel lifting" OR "hensle lifting") rsa exponent
takagi rsa
rsa "public key" "private key" bit length bits
public key and private key same length

## ACM

+author:takagi +rsa
+rsa +hensel
+rsa "chinese remainder" crt

## IEEE

(takagi <in> au) <and> rsa
rsa <and> hensel
rsa <and> ("chinese remainder" <or> crt)

## Other

| Search tool | Search Terms |
|---|---|
| webcrawler (with date restriction) | RSA "chinese remainder" public private |

**Applications/Patents from Inventor Search**

60/211,023
60/511,031
60/223,171
60/259,786
09/877,302
09/901,350
60/307,672